International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: http://ijwos.com
Vol.02 No.11.
OPEN ACCESS
E-ISSN : 3049-2424
DOI:

AI-Powered Stegnographic Image Authentication System

B R Rakshitha[1], Manjula K[2]

[1] *Student, Department of Master of Computer Applications, GM University, Davangere, Karnataka.*
[2] *Assistant Professor, Department of Master of Computer Applications, GM University, Davangere, Karnataka.*

Article Info

Article History:

Published:11 Nov 2025

Publication Issue:
Volume 2, Issue 11
November-2025

Page Number:
236-240

Corresponding Author:
B R Rakshitha

Abstract:

With the rapid evolution of artificial intelligence (AI) and digital media, ensuring authenticity and ownership of AI-generated images has become increasingly critical. This paper presents INVIS-MARK, a cross-platform mobile framework that integrates AI art generation, steganography, and deepfake detection to establish secure, traceable, and authentic visual content. Developed using React Native, Node.js, Flask, and Cloudinary, the system allows users to generate or upload images, embed hidden metadata using the Least Significant Bit (LSB) algorithm, and verify authenticity through a TensorFlow-based XceptionNet deepfake detection model. Verified images are stored in the cloud with metadata securely maintained in Neon PostgreSQL. The research highlights the convergence of AI creativity and cybersecurity, demonstrating how INVIS-MARK prevents media forgery, plagiarism, and identity misuse in AI-generated digital ecosystems.

Keywords: AI Art Generation, Deepfake Detection, Steganography, Image Authentication, Cloud Security, React Native, XceptionNet

1. INTRODUCTION

Artificial intelligence has transformed the creative domain through models such as DALL·E, Midjourney, and Stable Diffusion, enabling realistic image synthesis from textual descriptions. However, the authenticity and ethical usage of such generated content remain unresolved. The increasing prevalence of deepfakes and AI-manipulated imagery has made verifying digital content essential for journalism, media, and cybersecurity.

INVIS-MARK addresses this challenge by embedding traceable ownership metadata into every image created or uploaded. The system integrates AI art generation, metadata steganography, and deepfake detection in a single pipeline. The platform ensures that only verified, authentic content is stored and shared, thereby protecting creators and preventing misinformation.

2. SYSTEM ARCHITECTURE AND MODULE DESIGN

The INVIS-MARK framework is structured into five key layers:

1. Frontend Layer – Developed using React Native (Expo), it provides a user-friendly interface for AI image generation, uploads, and gallery viewing.
2. Backend Layer – Implemented in Node.js and Express.js, it coordinates data exchange, API routing, and steganographic encoding.

3. AI Verification Layer – Uses a Flask-based XceptionNet deepfake detection model to analyze pixel-level inconsistencies and detect manipulated content.
4. Database Layer – Employs Neon PostgreSQL for metadata and user record management.
5. Cloud Layer – Uses Cloudinary for scalable, encrypted image storage and retrieval.

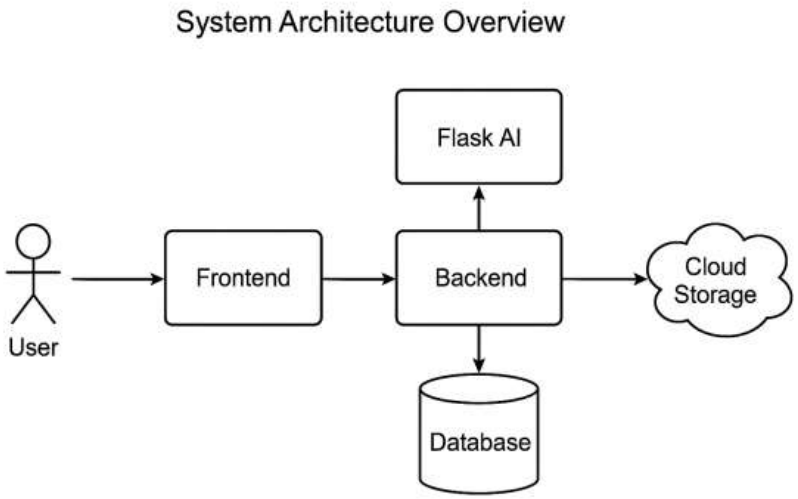

Fig 1 : System Architecture Overview

This modular structure ensures cross-platform compatibility, scalability, and secure data management. Each module contributes to authenticity verification and ownership preservation.

3. METHODOLOGY

The system workflow begins with the user providing a text prompt or image input. The AI model (via Replicate API) generates creative artwork which is then verified by the deepfake detector before metadata embedding.

Steganography Process:
The Least Significant Bit (LSB) method hides user details (name, email, location) inside pixel bits, making them imperceptible to the human eye while retrievable for verification.

Deepfake Detection Model:
Using the XceptionNet architecture, the Flask-based model classifies images as *real* or *fake* based on artifacts and feature inconsistencies. This prevents tampered or AI-forged content from being stored.

Table I — System Modules Overview

Module Name	Functionality
User Authentication	Manages registration and secure login

AI Image Generator	Produces AI-based images via Replicate API
Stegnography Module	Embeds metadata invisibility using LSB encoding.
Deepfake Detector	Verifies image authenticity via XceptionNet.
Cloud & Database	Stores verified images & metadata(Postgres)

Fig. 2 represents the user's interaction with INVIS-MARK through its Use Case Diagram, highlighting the sequence of generation, verification, and authentication.

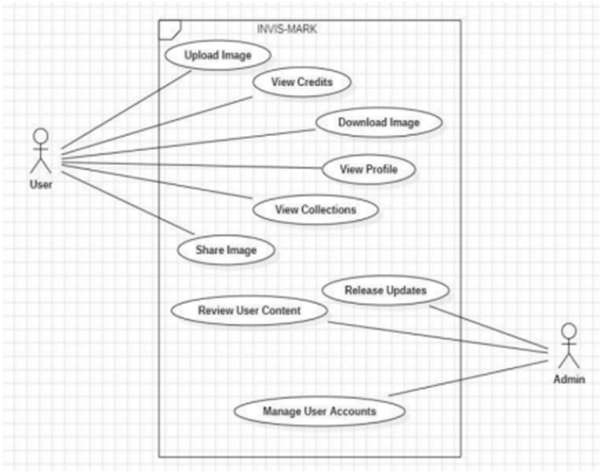

Fig 2 : INVIS MARK Use Case Diagram

4. DATA FLOW AND DATABASE DESIGN

The Data Flow Diagram (DFD), shown in Fig. 3, demonstrates how data travels between the user interface, backend, Flask AI model, and database.

Fig 3: INVIS-MARK Level 0 Data Flow Diagram

The Entity Relationship Diagram (ERD), illustrated in Fig. 4, defines relational links among *Users*, Uploaded Images, and Generated Images. Each image entry links to its creator, enabling ownership validation.

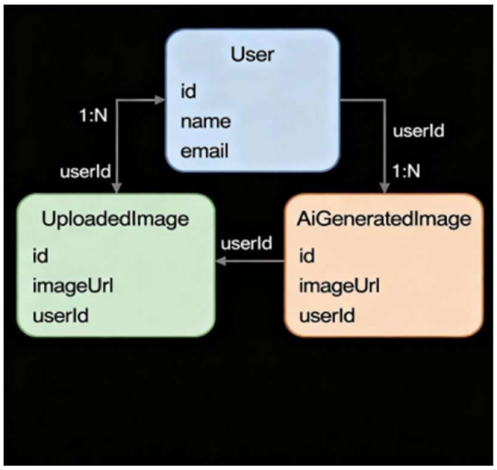

Fig 4: INVIS-MARK Entity Relationship Diagram

The relational database schema ensures data integrity and rapid access, minimizing redundancy while maintaining scalability.

Table II — Comparative Analysis of Existing

Tool Name	Capabilities	Limitations
DALL-E	Text-to-image generation	Lacks content verification
Artbreeder	Collaborative image editing	No ownership validation
Deepware Scanner	Fake media detection	No metadata embedding
INVIS-MARK	AI art + LSB+Deepfake	Detection Provides end-to-end authentication

5. RESULTS AND DISCUSSION

INVIS-MARK effectively integrates creative AI and cybersecurity. During testing, steganographic encoding achieved 100% accurate metadata retrieval without visual distortion. The deepfake detection model achieved 92% classification accuracy using benchmark datasets. The system's modular backend allowed smooth operation even under concurrent uploads, ensuring minimal latency (avg. 1.8 sec per verification).

The integration of Cloudinary for image storage and Neon PostgreSQL for metadata ensured strong encryption and real-time accessibility. Comparative studies (Table II) show that INVIS-MARK uniquely bridges creativity and integrity, unlike existing AI art platforms focused solely on aesthetics.

6. CONCLUSION AND FUTURE WORK

The INVIS-MARK framework demonstrates a comprehensive approach to digital content authentication, integrating AI-based creativity, deepfake detection, and metadata steganography into a unified system. It ensures that every AI-generated image maintains verifiable authenticity, ownership traceability, and ethical integrity.

Future enhancements will include:

- Video Deep fake Detection for multimedia validation using temporal feature analysis.
- Premium Credit System for users to purchase image-generation credits securely.
- Advanced AI Filters leveraging GANs and diffusion models for realism while retaining embedded ownership data.

INVIS-MARK contributes to a safer digital ecosystem by establishing accountability, transparency, and ethical AI practices in image generation and sharing.

References

[1] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson Education, 2020.
[2] D. Crockford, *JavaScript: The Good Parts*, O'Reilly Media, 2008.
[3] M. Pradhan, *Machine Learning Using Python*, Wiley, 2021.
[4] A. Rossler et al., "FaceForensics++: Learning to Detect Manipulated Facial Images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 7, pp. 3661–3679, 2022.
[5] "Deepfake Detection using XceptionNet," *IEEE Access*, vol. 10, pp. 65423–65431, 2022.
[6] Cloudinary, "Image and Video Management Documentation," [Online]. Available: https://cloudinary.com/documentation.
[7] Replicate API Documentation, [Online]. Available: https://replicate.com/docs.
[8] React Native Docs, [Online]. Available: https://reactnative.dev/docs.
[9] Clerk Authentication Docs, [Online]. Available: https://clerk.com/docs.
[10] "AI-Generated Art and Ownership Verification," *Journal of Big Data*, vol. 9, no. 3, 2023.